IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

MILAGROS CHATELAIN, individually and on behalf of all others similarly situated, Plaintiff, v. UNIVERSITY OF MINNESOTA, Defendant.	Case No. CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Milagros Chatelain ("Plaintiff"), individually and on behalf of all others similarly situated (collectively "Class Members"), by and through her attorneys, brings this Class Action Complaint against Defendant University of Minnesota ("Defendant" or "UMN"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against UMN for its failure to secure and safeguard the personally identifiable information ("PII") approximately 7 million people.[1]

[1] *See* Dana Thiede & Lou Raguse, *U of M Investigating Claimed Data Breach*, Kare11 News (Aug, 22, 2023), *available* at https://www.kare11.com/article/news/local/u-of-m-investigating-claimed-data-breach/89-17a1736f-a704-4495-9337-079e0c77ccd5 (last accessed Sept. 29, 2023).

2. UMN is a public research university with multiple campuses throughout the State of Minnesota. UMN is the oldest and largest in the University of Minnesota system and has the ninth-largest main campus student body in the United States, with more than 50,000 students annually. Upon information and belief, UMN has over 50,000 students and 485,000 living alumni.[2] UMN claims to be "[a]n [i]ndispensable [e]ngine for Minnesota" that "contributes more than $8.6 billion a year in economic activity to the state.[3]

3. In connection with their participation in the services and operations of UMN, students, prospective students, employees, applicants, and others affiliated with the UMN ("Class Members") provide it with highly sensitive personal information, including PII including, among other things, names, addresses, telephone numbers, email addresses, and Social Security numbers. UMN gathers this information and stores it on its servers in a database.

4. On August 22, 2023, the University of Minnesota sent an email to all faculty, staff, and students informing them that "the University became aware that an unauthorized party claimed to be in possession of sensitive data allegedly taken from the University's systems."[4]

5. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII

---

[2] *See About Us*, UNIVERSITY OF MINNESOTA, https://twin-cities.umn.edu/about-us (last visited, Sept. 29, 2023).
[3] See i*d.*
[4] *See University of Minnesota: Notice of Data Incident*, UNIVERSITY OF MINNESOTA, https://system.umn.edu/data-incident (last accessed Sept. 29, 2023).

through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

6. As a public research university, UMN knowingly obtains sensitive PII from students, employees, applicants, and others affiliated with the UMN and has a resulting duty to securely maintain such information in confidence. UMN owed a non-delegable duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. It also had an obligation to ensure that any vendor or third party it selected to offload the sensitive information it was entrusted with would take reasonable measures to safeguard that data.

7. Based on the public statements of UMN to date, a wide variety of PII was implicated in the Data Breach, including, but not limited to, names, birthdates, Social Security numbers, and driver's license or passport information.[5]

8. Unlike financial information, such as credit card and bank account numbers, the PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and Social Security numbers are given at birth and attach to a person for the duration of his or her life.

[5] *See id.*

For these reasons, these types of information are among the most lucrative and valuable to hackers.

9. As a direct and proximate result of UMN's failure to adequately safeguard the sensitive data entrusted to it (and failure to abide by its own Privacy Policy) Plaintiff's and Class Members' PII has been accessed by "unauthorized actors."[6]

10. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Indeed, Plaintiff has already been subject to attempted identity theft. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

11. Plaintiff, on behalf of herself and the Class as defined herein, bring claims for negligence, negligence *per se*, breach of fiduciary duty, breach of an implied contract, breach of contracts to which Plaintiff is an intended third party beneficiary and, in the alternative, unjust enrichment.

PARTIES

Plaintiff

12. Plaintiff Milagros Chatelain is a current resident of New Rochelle, New York. Plaintiff Chatelain applied to attend school as an undergraduate at the UMN in 2012.

[6] *See id.*

In her application, she provided UMN with her PII, including her name, contact information, Social Security number, and date of birth, among other information. Plaintiff Chatelain was a prospective student for UMN but did not attend UMN as an undergraduate. Plaintiff Chatelain received an email from UMN that her sensitive PII was involved in the Data Breach.

Defendant

13. Defendant UMN is a higher education public institution in the State of Minnesota that accepts applicants to its undergraduate and graduate programs from people throughout the United States and from non-U.S. born individuals. It, furthermore, employs thousands of staffs in academic and non-academic roles.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, minimal diversity is met under CAFA because at least one member of the proposed Class is diverse from the Defendant. UMN is located and operates exclusively in the State of Minnesota and is a citizen of only that State. The Class is comprised of applicants to attend UMN, and current and former students and employees of UMN, which includes individuals dispersed throughout the country and who are citizens

of States other than Minnesota. Plaintiff alleges that, in the aggregate, the claims of all putative class members exceed $5,000,000, exclusive of interest and costs.

15. This Court has general personal jurisdiction over UMN because UMN is located entirely within the State of Minnesota and is a Minnesota public institution operating on behalf of the State of Minnesota. UMN has minimum contacts with Minnesota because it is located there and conducts substantial business there, and Plaintiff's claims arise from UMN's conduct in Minnesota, including because UMN's database containing the information stolen is located in Minnesota.

16. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in Minnesota and because UMN conducts a substantial part of its business within this District.

FACTUAL BACKGROUND

A. UMN and the Services it Provides.

17. UMN is public research university that has more than 50,000 students annually, 485,000 living alumni, and 20,000 faculty and staff that help operate UMN, which claims to contribute "more than $8.6 billion a year in economic activity" to the state of Minnesota.

18. In the course of its operations, UMN comes into the possession of the highly sensitive PII of Plaintiff and Class Members. Plaintiff and Class Members entrusted this information to UMN with the reasonable expectation and mutual understanding that it

would comply with its obligations to keep such information confidential and secure from unauthorized access.

19. UMN recognizes the importance of protecting this data. Indeed, it admits to being governed by the Minnesota Government Data Practices Act and cannot release personally identifying information without consent.[7] UMN has also implemented policies and procedures regarding its expected behavior in the case of a "Data Security Breach," which states that it "will provide timely and appropriate notice to affected individuals when there has been a breach of security involving private data about them."[8] Further, under Minn. Stat. § 13.05, subd. 5(2) of the Minnesota Government Data Practices Act, entities like UMN must "establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only accessed by those persons for purposes described in the procedure."

20. By obtaining, collecting, and storing Plaintiff and Class Members' PII, UMN assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiff's and Class Members PII from unauthorized disclosure.

21. UMN nevertheless employed inadequate data security measures to protect and secure the PII clients entrusted to it, resulting in the Data Breach and compromise of

[7] *Privacy Statement*, UNIVERSITY OF MINNESOTA, https://twin-cities.umn.edu/privacy (last accessed Sept. 29, 2023).
[8] *See Data Security Breach: Policy Statement*, UNIVERSITY OF MINNESOTA, https://policy.umn.edu/it/securitybreach (last accessed Sept. 29, 2023).

Plaintiff's and Class Members' PII. Individuals entrusted UMN with their sensitive data of PII, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII.

B. UMN Knew the Risks of Storing Valuable PII and the Foreseeable Harm to its Clients.

22. At all relevant times, Defendant knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

23. Defendant also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private health information.

24. Defendant stores, maintains, and uses Plaintiff's and Class Members' Private Information.

25. Defendant maintains a "University database" to store Plaintiff's and Class Members' Private Information. Defendant utilized the database with complete disregard for its data security and infrastructure.

26. Defendant agreed to and undertook legal duties to maintain the Private Information of Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws. Defendant had obligations created by the FTC Act, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

27. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential

attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[9]

28. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[10]

29. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's clients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

30. PII is a valuable property right.[11] The value of PII as a commodity is measurable.[12] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal

[9] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[10] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Sept. 26, 2023).

[11] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[12] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle./824192.

and regulatory frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

31. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

32. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[15]

---

[13] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[14] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[15] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Sept. 26, 2023).

33. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

34. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites." [16]

35. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

36. Based on the value of its clients' PII to cybercriminals and cybercriminals' propensity to target healthcare providers, UMN certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

[16] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

C. Defendant Breached its Duty to Protect its Clients PII

37. On July 15, 2023, a tech blog, thecyberexpress.com, reported on a potential UMN data breach by way of a "post on the dark web" in which "a hacker claimed to have accessed the University of Minnesota data warehouse containing records since 1989 and extracted information including 7 million unique social security numbers."[17]

38. Defendant allegedly learned on July 21, 2023 that a person was claiming to have posted on the Internet in July 2023 certain admissions, race, and ethnicity information held in a University database.[18]

39. According to UMN, it immediately initiated an investigation and promptly engaged forensics professionals to assess whether the claim was credible and to ensure the security of the University's electronic systems.[19]

40. After determining that a person likely gained unauthorized access to a University database in 2021, the investigation confirmed that the PII may have been accessed or acquired by an unauthorized third party.[20]

41. Upon information and belief, on August 22, 2023, over a month after UMN learned of the Data Breach, UMN began to send notices out to impacted individuals.[21]

---

[17] *See U of M Investigating Claimed Data Breach, supra.*
[18] *University of Minnesota: Notice of Data Incident, supra.*
[19] *Id.*
[20] *Id.*
[21] *Id.*

42. The PII compromised in the Data Breach includes names, addresses dates of birth, Social Security numbers, driver's license or passport numbers, financial account and/or payment information, medical information, and health insurance information.[22]

43. Like Plaintiff, the Class Members received similar notices informing them that their PII was exposed in the Data Breach.

44. All in all, 7 million individuals had their PII breached.[23]

45. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its clients' PII.

46. Plaintiff and Class Members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including PII;

b. Improper disclosure of their Private Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

d. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves may use that information to defraud other victims of the Data Breach;

[22] *Id.*
[23] *See U of M Investigating Claimed Data Breach, supra*.

e. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach; and

f. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' personal information for which there is a well-established and quantifiable national and international market.

D. FTC Guidelines Prohibit UMN from Engaging in Unfair or Deceptive Acts or Practices

47. UMN is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

48. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

49. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal

[24] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[25]

50. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. UMN failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

---

[25] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformationpdf.

[26] *Id.*

53. UMN was at all times fully aware of its obligations to protect the PII of its clients, which gave it direct access to reams of patient PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

54. Cyberattacks and data breaches at companies like UMN are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

55. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[27]

56. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example,

[27] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

57. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

58. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[28]

59. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit

[28] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 24, 2023).

card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

60. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

61. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[29]

62. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

[29] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

63. As discussed above, PII is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

64. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [30]

65. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[31]

66. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[32] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[33] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social

---

[30] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).
[31] *Id.*
[32] *Id.*
[33] *Id.* at 4.

Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

67. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[34]

68. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like UMN is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

69. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[35] "[I]f there is reason to believe that your personal

[34] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.
[35] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

information has been stolen, you should assume that it can end up for sale on the dark web."[36]

70. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[37]

71. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

72. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[38]

73. Cybercriminals can post stolen PII on the cyber black-market for years following a data breach, thereby making such information publicly available.

---

[36] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[37] *Id.*

[38] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

74. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [39] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[40]

75. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[41]

76. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

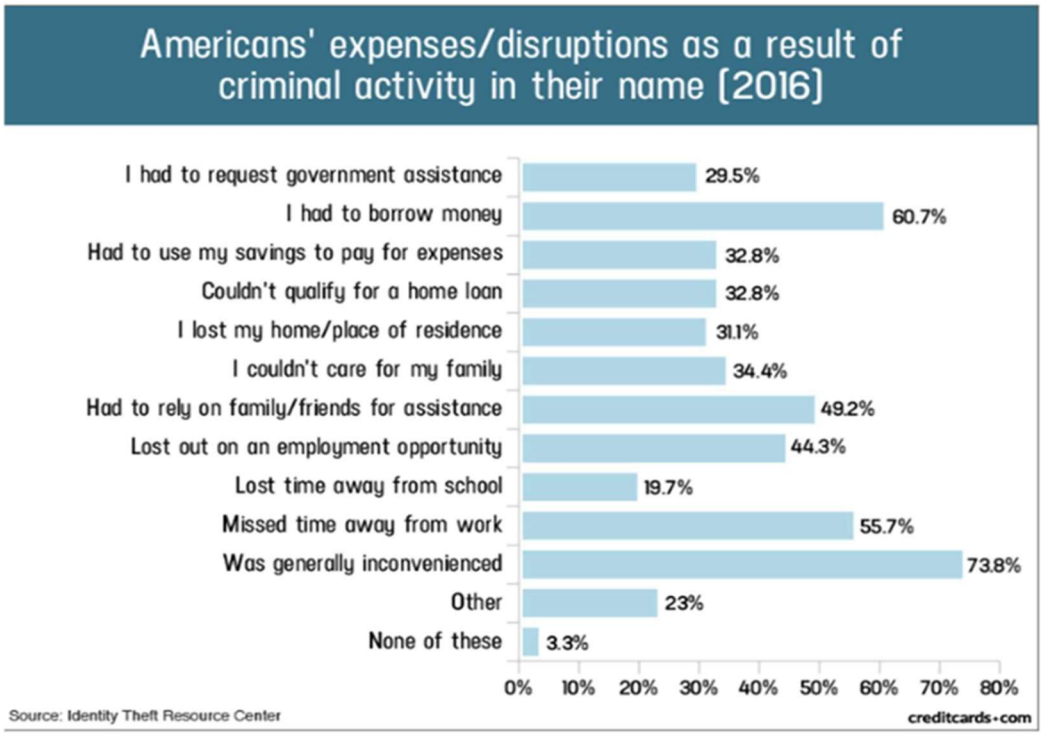
77. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.

---

[39] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Sept. 26, 2023).

[40] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Sept. 26, 2023).

[41] *Guide for Assisting Identity Theft Victims*, Fed. Trade Comm'n, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.



78. Victims of the Data Breach, like Plaintiff and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[42]

79. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and

[42] *Id.*

closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

80. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which remains in the possession of UMN, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. UMN has shown itself to be wholly incapable of protecting Plaintiff's and Class Members' PII.

81. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to UMN is removed from Defendant's unencrypted files.

82. UMN acknowledged, in its letter to Plaintiff and Class Members, that, in response to the Data Breach, UMN "has also taken steps to bolster its overall system security."[43]

F. Plaintiff and Class Members Suffered Damages

83. In requesting and maintaining Plaintiff's PII for business purposes, UMN expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's PII. UMN did not, however, take proper care of Plaintiff's PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

[43] *See University of Minnesota: Notice of Data Incident, supra.*

84. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and members of the Class must devote time, energy, and money to monitor and mitigate their risk of fraud. Plaintiff has taken or will likely be forced to take these measures in order to mitigate her potential damages as a result of the Data Breach.

85. Once PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

86. Further, the value of Plaintiff and Class Members' PII has been diminished by its exposure in the Data Breach.

87. Plaintiff and Class Members would not have provided their PII to UMN had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII from criminal theft and misuse.

88. As a result of Defendant's failures, Plaintiff and Class Members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII.

89. Further, because Defendant delayed in notifying Plaintiff and the Class about the Data Breach for over two months, Plaintiff was unable to take affirmative steps during that time period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

90. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[44]

91. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its clients PII.

92. In addition, Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud.

G. Plaintiff's Experiences

93. Plaintiff Chatelain received a data breach notice from Defendant dated September 25, 2023 informing her that "the security of some private information that the University of Minnesota maintains about [Chatelain]" was potentially compromised during the Data Breach. Specifically, UMN informed Plaintiff that her Social Security number, driver's license number, and other information had been compromised during the Data Breach.

[44] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Sept. 26, 2023).

94. Plaintiff Chatelain takes care to protect her PII. Had Plaintiff Chatelain known UMN would not adequately protect the PII/PHI entrusted to it, she would not have entrusted her PII with UMN or agreed to provide UMN with her PII. As a direct result of the Data Breach, Plaintiff Chatelain has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII; and deprivation of the value of her PII.

95. She has also spent significant time monitoring her accounts for fraudulent activity, and will need to do so for the foreseeable future. Plaintiff Chatelain plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

CLASS ALLEGATIONS

96. Pursuant to Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff seeks certification of a Class as defined below:

> All individuals whose PII and was compromised in the UMN Data Breach, which was announced on or about August 22, 2023 (the "Class").

97. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

98. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or

when they move for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

99. **Numerosity:** The Class Members are so numerous that individual joinder of all Class Members is impracticable. UMN estimates that approximately 600,794 individuals were affected by the Data Breach. All Class Members' names and addresses are available from UMN's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

100. **Commonality:** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Defendant failed to timely notify Plaintiff and Class Members of the Data Breach;

b. Whether Defendant had a duty to protect the PII of Plaintiff and Class Members;

c. Whether Defendant was negligent in collecting and storing Plaintiff and Class Members' PII, and breached its duties thereby;

d. Whether Defendant breached its fiduciary duty to Plaintiff and the Class;

e. Whether Defendant breached its duty of confidence to Plaintiff and the Class;

f. Whether Defendant entered a contract implied in fact with Plaintiff and the Class;

g. Whether Defendant breached that contract by failing to adequately safeguard Plaintiff's and Class Members' PII;

h. Whether Defendant was unjustly enriched;

i. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

j. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

101. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all clients of Defendant, each having their PII exposed and/or accessed by an unauthorized third party.

102. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class Members. Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

103. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to

Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class Member suffered damages by that conduct.

104. **Superiority:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like UMN. Even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

105. Finally, all members of the proposed Class are readily ascertainable. Defendant had access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach.

106. Unless a class-wide injunction is issued, UMN may continue to maintain inadequate security with respect to the PII of Class Members, UMN may continue to refuse to provide proper and adequate notice to Class Members regarding the Data Breach, and UMN may continue to act unlawfully.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

107. Plaintiff restates and realleges the preceding allegations of the paragraphs above as if fully alleged herein.

108. Plaintiff brings this claim individually and on behalf of the Class.

109. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, and control.

110. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

111. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

112. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their

Private Information that was in Defendant's possession. As such, a special relationship existed between the Defendant and the Plaintiff and Class Members.

113. Defendant were aware of the fact that cyber criminals routinely target corporations through cyberattacks in an attempt to steal the Private Information of employees, applicants, business associates, customers, and patients.

114. Defendant breached the duties owed to Plaintiff and Class Members and thus were negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiff's and Class Members' PII, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur:

(a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its consumers; and (h) failing to adequately train and

supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

115. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

116. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

117. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

118. Plaintiff restates and realleges the preceding allegations of the paragraphs above as if fully alleged herein.

119. Plaintiff brings this claim individually and on behalf of the Class.

120. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by

entities such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

121. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving PII of its clients.

122. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

123. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

124. As a direct and proximate result of Defendant's negligence, Plaintiff's and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and The Class)

125. Plaintiff restates and realleges the preceding allegations of the paragraphs above as if fully alleged herein.

126. Plaintiff brings this claim individually and on behalf of the Class.

127. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

128. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

129. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased business services from Defendant and/or its agents and in so doing, provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

130. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

131. In particular, Defendant enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

132. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because

Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

133. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

134. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

135. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

136. Plaintiff and Class Members have no adequate remedy at law.

137. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and

identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

138. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

139. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they

unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FOURTH CAUSE OF ACTION
VIOLATION OF THE GOVERNMENT DATA PRACTICES ACT, MINN. STAT. CH. 13. (MNGDPA)
(On Behalf of Plaintiff and The Class)

140. Plaintiffs repeat and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

141. Under the MNGDPA, a government entity that "violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damages as a result of the violation, and the person damaged . . . may bring an action against the responsible authority or government entity to cover any damages sustained, plus costs and reasonable attorneys fees." Minn. Stat. § 13.08, subd. 1. Furthermore, "[t]he state is deemed to have waived any immunity to a cause of action brought under this chapter." *Id.* Additionally, the MNGDPA states that "[a] responsible authority or government entity which violates or purposes to violate this chapter may be enjoined by the district court." *Id.* at subd. 2.

142. The MNGDPA governs UMN and applies to its storage of Plaintiff's and the Class's personal information. Minn. Stat. § 13.01, subd. 1 ("All governmental entities shall be governed by this chapter.").

143. Under the MNGDPA, UMN was required to "establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment

reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure." Minn. Stat. § 13.05, subd. 5(a)(2). 86. Furthermore, the MNGDPA required UMN to obtain annual security assessments of any personal information maintained by the government entity. *Id.* at § 13.055, subd. 6. Highlighting the significance of protecting data against unauthorized disclosure, when a breach does occur, the MNGDPA requires government entities to notify impacted individuals "in the most expedient time possible and without unreasonable delay . . . ." Id. at subd. 2(a).

144. UMN acknowledges its obligations to protect data under the MNGDPA, indicating that it is well aware of the importance of security data against unauthorized access.

145. However, UMN failed to adopt "appropriate security safeguards" to protect Plaintiff's and the Class's highly sensitive information that it stored in its database. The lack of appropriate security safeguards is made clear by the means by which the Data Breach occurred. Specifically, a single hacker with no apparent history of orchestrating data breaches as part of a cybercrime organization singlehandedly infiltrated UMN, obtained control over its networks and access to its databases, successfully exfiltrated a massive amount of data involving over seven million individuals, and exfiltrated that data all without detection. UMN had no idea it had been breached and the data on its databases stolen until the hacker publicly disclosed the breach and, by the time UMN began investigating it, the hacker, having succeeded in obtaining a swath of valuable data, had already ceased activity within UMN's networks and servers. UMN, therefore, violated the MNGDPA.

146. Plaintiff, furthermore, suffered damages as a result of the Data Breach, which occurred directly because of UMN's violation of the MNGDPA and its failure to adopt appropriate security safeguards.

147. Specifically, Plaintiff's and the Class's highly sensitive information has been placed on the dark web where cybercriminals have access to it and opportunity to misuse it. Consequently, the confidentiality, integrity, and value of this sensitive information has been diminished because it can no longer guarantee Plaintiff and the Class's identities. Plaintiff and the Class were also damaged due to the need to expend time, effort, and money monitoring their financial accounts, social media applications and their credit scores to identify any misuse of their data. Plaintiff, in fact, remained at a heightened and substantial risk of harm due to the misuse of her data which has been placed directly in the hands of criminals. Finally, Plaintiff suffered emotional distress stemming from the disclosure of her sensitive data and the heightened and prolonged risk of harm she now suffers.

148. A private individual who acted as UMN did under the circumstances alleged herein would be liable to Plaintiff and the Class.

149. Plaintiff, therefore, seeks to recover the damages she suffered and costs and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

a. For an order certifying the Class as defined herein, and appointing Plaintiff and her counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Respectfully submitted,

Dated: October 2, 2023

/s/ Brian C. Gudmundson

Brian C. Gudmundson (MN Lic. #336695)
Michael J. Laird (MN Lic. #398436)
Rachel K. Tack (MN Lic. #399529)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Jonathan Shub
(*pro hac vice* forthcoming)
Benjamin F. Johns
(*pro hac vice* forthcoming)
Samantha E. Holbrook
(*pro hac vice* forthcoming)
SHUB & JOHNS LLC
Four Tower Bridge

200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

Attorneys for Plaintiff and the Putative Class